CyberSecurity and Digitalization in the Railway Domain

Digital Transport Days

DB Netz AG | Christian Schlehuber | I.NVI 62 | Helsinki | 2019-10-09

Introduction to Railway Systems

Biggest business premise in Europe – **with public access**
- Stations as gate to railway transportation
- Europe-wide rail networks

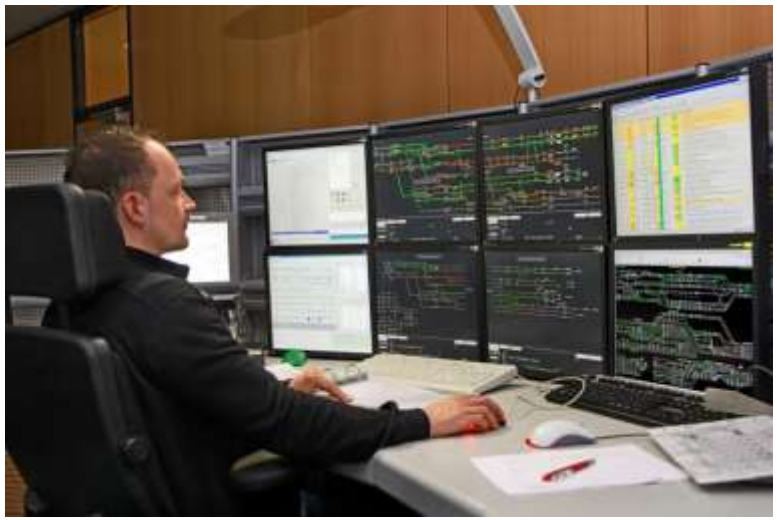
Strong regulations of technical installations (according Safety)
- EN 50126 (Reliability, Availability, Maintainability, Safety – RAMS)
- Etc.

➔ National Safety Authority has to grant **admission for every critical railway system**

➔ Categorized as **Critical Infrastructures** in most European countries

Evolution of transport
- Autonomous driving and platooning
- Flexible travel concepts (Uber, etc.)

➔ **Railways also have to evolve to keep track!**



How does this evolution look like? Digitalization in Rail

Main technologies and solutions “responsible” for acceleration of digital transformation:

- Automation (ATO), Level 3, Sat localization
- Big Data Analytics, Artificial Intelligence (AI)
- Internet of (Every)Thing (IoT)
- Cloud Computing, etc.

Adaption of these technologies as INDUSTRY 4.0 and/or RAILWAY 4.0:

- Digital/Automation train control (ATO)
- Digital signaling and traffic management
- Digital (predictive) maintenance
- Mobile apps, e-ticketing, etc.
- “Datacenter on wheels”

(Not only) “Digital” Challenges for CyberSecurity

- Railway technologies are sector specific and split into **Signaling, Rolling Stock and Fixed Installations**
- Systems have a **lifetime of 30+ years and approval is required**
- **Digitalization** initiatives move Infrastructure towards intelligent, more connected, more assisted systems
- **Obsolescence** of Safety systems exposed to current and future cyber threats landscape
- **Standards** for Railways currently **not up to date with CyberSecurity** challenges
- **Awareness** not at a desired level

Solutions

- **CENELEC Working Group 26 develops a CyberSecurity Standard** for the Railway Domain
  - Final version expected mid/end of 2020
  - European and national authorities involved

- **European Rail Information Sharing and Analysis Center** (ER-ISAC) ramping up since 10/2018
  - Sharing on Security Architectures and Best-Practices
  - Development of Security Baselines
  - Information Sharing on current Incidents

- **Collaboration** with European Institutions
  - CyberSecurity Workstream of the Digitizing Steering Group for Railways
  - ENISA focusing more on the Railway Domain
  - Research on CyberSecurity topics within Shift2Rail

Thank you for your attention

M.Sc. Christian Schlehuber
Lead of CyberSecurity R&D

DB Netz AG
I.NVI 62
Weilburger Str. 22
60326 Frankfurt am Main

Phone: +49 152 – 3753 7938
christian.schlehuber@deutschebahn.com
www.deutschebahn.com

http://fahrweg.dbnetze.com